Measuring Results at the NSA

JAMES F. MISKEL

"When I heard that I would be coming to the National Security Agency or NSA, I decided to read the book *Crypto* by Steven Levy because it had been recommended to me as an excellent study of how NSA dealt with technological trends in the 1980s and 1990s. After listening to you describe the recent reorganization at the NSA, it strikes me that we've come full circle. This reorganization looks a lot like the structure that the Levy book said the NSA had when it was first established under President Truman," Captain Bill Basie (USN) observed to the briefer who had been assigned to give him and some other new employees the basic 'This is NSA' briefing.

Indeed, as the briefer acknowledged, when the NSA was formed in 1952 the agency had been organized into two major divisions: Communications Security and Communications Intelligence.[1]

The focus of communications security or COMSEC was the protection of United States communications through the use of codes that eavesdroppers can't break. The COMSEC function has changed considerably since then, but the challenge ultimately remains the same—insuring that classified and other important information is protected from potential adversaries, including criminals and hackers. Hence the name of the new division: Information Assurance.

Communications intelligence, or COMINT, involved eavesdropping on the communications of our adversaries and potential adversaries. Sometime between 1952 and the 1980s the term signals intelligence, or SIGINT, displaced COMINT in the national security lexicon, presumably as a result of the digitalization of communications and the development of new communications technologies like satellites and wireless phones. In any event, the name of the second of the two major NSA divisions was Signals Intelligence.

The briefer went on to explain that prior to December 2000, the NSA had been organized into five directorates. In addition to the SIGINT and COMSEC Directorates, there were directorates for Technology, Policy, Budget, and Support. It struck Captain Basie that the five-directorate structure seemed to place core competencies and support functions on a par with each other. He wondered if the new two-directorate structure reflected a judgment that too much emphasis had been placed on support functions and not enough on the principal missions. He decided to do a little research on that topic while he settled in to his new job in the office of the NSA's chief of staff.

The position of chief of staff was itself a new fixture on the NSA organizational chart. It was located in the Office of the Director and was headed by a Navy admiral, Oscar Peterson. NSA had both civilian and military employees. The director and some other key positions were military, but most of the senior slots were civilian and most of the civilians were long-time employees of the agency.

Basie's first day on the job started with a get-acquainted meeting with Admiral Peterson. Peterson confirmed to Basie that the NSA leadership felt that the old five-division structure had dissipated the focus on the primary missions of information assurance (a.k.a. COMSEC and SIGINT).

"The NSA is facing some serious challenges that we really need to focus on. Some of those challenges are technological; some are political; some are economic, " Admiral Peterson explained.[2]

"The technological challenges exist in both the information assurance and SIGINT realms. It is getting a lot more difficult to protect important communications and data transfer systems from information attack. Here's an example. Hackers shut down Microsoft's internet sites for five hours on January 25, 2001.[3] Microsoft has extremely talented programmers and great financial incentives to protect their systems, yet hackers managed to bring them down. Imagine the damage that could be caused if someone brought down a secure Defense Department system during a crisis! Remember the so-called Love Bug virus in 2000 and all the damage it caused? We are trying to shield national security systems from these types of threats. We are also in the business of blocking attempts by other powers to read our mail—to eavesdrop on classified communications or to get access to information in secure databases."

Admiral Peterson paused to pour himself a cup of coffee and to offer Captain Basie one and then continued, "So much of our economy depends upon digitized information that we find ourselves also involved in setting standards for private sector data protection. In the old days we tried to discourage the private sector from getting into the data encryption game. For obvious reasons, NSA did not want sophisticated encryption programs to be exported to countries whose signals we were interested in intercepting. For equally obvious reasons, the Federal Bureau of Investigation (FBI) supported us in the White House and in Congress. The FBI did not want criminals in the United States to have easy access to leading edge encryption programs. But the reality was that we could not keep the encryption genie in the bottle. And now that the genie is out of the bottle, it's getting a whole lot harder to interpret and analyze the stuff we collect through SIGINT.

"The government did not, much to our surprise," Admiral Peterson intoned with a hint of sarcasm, "have a monopoly on brains—cryptographers in the private sector started inventing and then selling their own solutions to data protection and their solutions were very good. Some private sector cryptographers have even made their programs available for free by posting them in downloadable form on the internet.[4] Then as the internet blossomed and electronic fund transfers, credit cards and automated teller machines (ATM) proliferated, corporations started to view encryption as essential to business. And the public started to see encryption as a method of ensuring their right to privacy. Encryption enabled people to withdraw cash from ATM machines, to use their credit cards to buy gasoline and groceries and to purchase books over the Internet without fear of someone stealing their credit card numbers."

"Our political challenges," the admiral continued, "are domestic and foreign. From the SIGINT perspective the end of the Cold War meant that our target set has changed dramatically. There is no Communist bloc to focus on. There instead are numerous terrorist groups, criminal organizations—like the drug cartels—and rogue states like Iraq, North Korea and the rump state of Yugoslavia under Milosevic. And then there are also states that are trying to develop weapons of mass destruction. Domestically, we are finding that Congress is a good deal less enthusiastic about our operations than it used to be. As you may know from reading the papers, NSA has been criticized in Congress for being slow to adapt to the 'brave new world' of high technology and asymmetric threats."[5]

"But enough of the background! Let me tell you about your first assignment. Implementing change in large, complex organizations like NSA is hard. It's real hard. NSA has a very strong culture that has proven to be quite resistant to change. As an agency, we depend heavily on highly talented scientists, linguists, mathematicians and others. If the people in these skill positions don't succeed in designing unbreakable codes or interpreting the encoded communications of our adversaries, we will fail as an agency and our military forces may suffer as a consequence. Yet if the skilled people don't adjust to the challenges NSA faces, the agency's ability to succeed in the future will be compromised.

"We have recently re-organized and we've taken a number of other steps that you'll need to learn about. But what differences will ultimately result?

"I subscribe to the old adage that 'you get what you measure'. I want you to do some research and give me advice about the measures we should use. Specifically, Captain Basie, I want your advice about the measures we should use to influence the performance of our people. What measures should we use to tell us whether we are succeeding in meeting the challenges that we face in information assurance and SIGINT?"

As he walked out of Admiral Peterson's office, Bill Basie decided to schedule appointments with senior staff in the information assurance and SIGINT directorates to get their ideas about measuring success and about measurements that might really influence how the agency operated and perhaps shape its culture. He also decided to learn more about the NSA front office by visiting with colleagues on the eighth floor of the agency headquarters building.

He quickly learned that the front office itself had recently been reorganized. Before December 2000 there really had been no strong Office of the Director structure. Some of the functions that had previously been performed by one of the former five-directorates had been shifted to the Office of the Director. Two examples were the functions performed by the chief financial manager and the chief information officer. The idea evidently was to allow the director to exert more control over "corporate" strategy. (Basie noticed that many of the folks he spoke with used the words "corporate" and "corporation". The words sounded odd coming from public sector types and military officers, but he surmised that the references were meant to reinforce thinking about NSA as a corporate whole—a single body.)

Another thing he quickly learned was that there had been a rather dramatic turnover in the senior levels of the agency within the past several months. Two things had happened. First, the director had reassigned some senior managers to less lofty posts inside the agency and had obtained "early out" authority for senior executive service (SES) employees. NSA already had early out authority for government service (GS) employees. So a lot of the old hands had left or were expected to leave. The second thing was that the director had brought in outsiders from industry and academia or promoted "young turks" to fill many of the leadership slots in the new organization.

One of the key outsiders was the chief financial manager. She was a former financial officer in the software industry. She was building an NSA-wide business plan and was improving the agency's cost accounting systems. Previously, the five directorates had formulated separate plans (annual plans about major expenditures) and the agency as a whole did not have a clear idea of how much individual support functions or cross-cutting projects actually cost. The other key outsider was Basie's own boss, Admiral Peterson who had not had a prior tour at NSA. Together the chief of staff and the chief financial manager were imposing discipline on the way in which the agency reached decisions and formulated its investment strategy.

One of the most dramatic aspects of the investment strategy was the decision by NSA leadership to outsource the upgrading of the agency's infrastructure—its computers and telecommunications hardware. A contractor or contractors were being hired to manage the ongoing hardware modernization effort for the entire agency—both the Information Assurance and SIGINT Directorates would be affected. It was a big-ticket project with big-ticket risks, although there were presumably risks inherent in any upgrade regardless of whether it was privatized or done in-house.

Basie's next round of meetings were with the "number twos" in the Information Assurance and SIGINT Directorates. Julian Adderley, the second in command of the Information Assurance outfit, started the interview by recounting the dramatic changes that had taken place in commercial cryptography in the past decade and the effects they had had on NSA.

"Our culture was formed at a time when NSA was the only supplier of information and communications security services. We might even have developed a touch of arrogance and complacency during those years and believe me, those attributes are hard to shake. Because we were the sole supplier, we got in the mode of reacting to specific customer requests, instead of pushing the envelope aggressively ourselves—educating the customer on what they might need to meet evolving threats," Adderley confided.

"We were risk averse. Because there was no competition, we could afford to put a high premium on perfection. We did not rush to market. We took our time to make damn sure that our encryption programs and hardware were foolproof. So we invested a lot in marginal improvements. Anyone who knows the software and computer industries today knows that is not consistent with commercial practices. New technologies and new software products are introduced much more quickly today.

"In order to succeed, the Information Assurance Directorate needs to do four things extremely well. The first is to decide what we should make by ourselves and what we should buy from others. The second is to do an outstanding job on the products and services we decide to develop in-house. The third is to set standards for commercial encryption and data protection products. The fourth is to understand where the technology will head in the future."

"The net result should be that in the future hackers won't be able to bring down government operating systems—like they did in 1998 when nine NASA field offices were crashed.[6] Another example of the threats we are trying to fend off involves the Defense Department's 'Eligible Receiver' exercise, in June 1997, in which two individuals simulated an attack in which they got access to data that they could have manipulated in ways that would have disrupted troop movements in a crisis.[7]

At this point in the discussion, Adderley called his military aid, Commander Sarah Vaughn, to join the discussion. Commander Vaughn was working on a project designed to strengthen NSA's relationships with industry. The relationships had been strained during the 1980s and 1990s because of NSA's ultimately unsuccessful efforts to prevent the exportation of highly sophisticated encryption technologies.

Vaughn started out by saying that despite past tensions, industry had an incentive to cooperate with NSA—at least the information assurance side of it. "After all, the United States government is the biggest customer for encryption products. Not only that, many other customers of encryption products might be reluctant to buy encryption products that the government is not happy with. For example, defense and aerospace industries might refuse to buy encryption products from a company that has fallen out of grace with the United States government, i.e., with NSA.

"We want to have a collaborative relationship with industry. We can't count any more on having the smartest cryptographers and mathematicians under the NSA roof. Now that there is a vibrant market for information assurance products, we have to compete with industry for the best brains. What with the differential in private and public sector salaries in some fields, we know that industry will win the competition often enough to ensure that many of the technological breakthroughs in the field will come from the private sector, not from NSA.

"We have started to consciously think of industry as a stakeholder, rather than an unruly competitor. Did Mr. Adderley tell you that we need to decide what things we really need to build ourselves and what things we should rely upon others to build?" After Basie nodded to indicate that Adderley had covered that ground , Vaughn continued.

"This is not just a question of divesting non-core competencies to focus on the highest value functions. Even the products that we don't build are going to be used by government agencies and by the private sector. If these products don't work, the results could be catastrophic for the affected agencies and companies. In other words, we have a stake in the success of the products that we decide not to build ourselves. So we try to set standards for the products we don't make. Here again, though, this is an area where we need to recognize the dissimilarity between government and industry approaches. As you know, industry wants to get products out the door as quickly as possible. Companies that spend too much time on marginal improvements might let the competition beat them to the marketplace. So these companies will not voluntarily comply with NSA standards that seem too demanding relative to the threat that the customer will ultimately face.

"We are evolving a three-tiered approach to the question of standards. For products intended for low risk environments (e.g., office software for an insurance company), NSA would articulate less demanding standards to which the makers of encryption products would be encouraged to adhere. More demanding standards would be articulated for information assurance products designed for the moderate risk environment faced by many government agencies and defense-related industries. For the high risk environment NSA would develop its own information assurance products.

"We also offer to run 'beta tests' on private sector products before they are released. For instance, in the past couple of months several of the largest software houses have sent us pre-release copies of the products to 'beta test', i.e., use in real world conditions. This is more or less what the makers of computer games do. To help find glitches, they send pre-release copies to some users who check the software out by playing the games."

The last stops on Basie's grand tour of the NSA were with the SIGINT deputy director, U.S. Air Force General A.C. Jobim, and one of the key civilian members of the SIGINT staff, Dr. John Coltrane. Jobim started the discussion by conceding that the Information Assurance folks had an easier time getting along with industry than Signals Intelligence folks did.

"Most of the fire that NSA has taken in the press and in Congress has, in recent years anyway, been more at SIGINT than information assurance. We've been unfairly criticized for spying on American citizens and our allies in Europe.[8] We have strict rules and procedures on the issue of intercepting domestic communications. This is an important boundary for us because we recognize how important it is for NSA to keep the trust of the American people and Congress. We don't have time to go into it now, but let me assure you that our procedures in this area are vigorously enforced—we've gotten great reviews whenever these procedures have been appraised by outside evaluators."

Basie knew that the SIGINT side of the house had also been criticized for being slow to react to the changes in the world—the new threats, the new technologies. He tried to steer General Jobim in the direction of the strategic challenges in the SIGINT area.

"As you know, our budget is included in the defense account and, like every Defense Department element, NSA has the challenge of balancing current readiness with investments in future capability. By readiness, I mean the ability to satisfy the demands our current customers—e.g., the CINCs, the White House—on an ongoing basis but also during a crisis," Jobim indicated.

"We think of SIGINT as consisting of three functions: getting important information, analyzing that information, and communicating the analysis to the customer. We need to do all three things well in order to succeed. Dr. Coltrane, one of our civilian PhDs, will tell you how we perform these functions during a crisis; then I'll discuss the routine, non-crisis functioning of the SIGINT directorate."

Dr. Coltrane gave Basie a succinct briefing on the National SIGINT Operations Center (NSOC) that NSA activates whenever there is a crisis. The NSOC sounded very much like the standard emergency operations center—a team of high-powered action officers with all the right connectivity inside and outside the NSA headquarters. Coltrane concluded the briefing by noting that, like other operations centers, there were always concerns about what happens when a fresh group of action officers is brought in to work on a crisis.

According to Dr. Coltrane, "Action officers who have not been assigned to the NSOC before, or who haven't been there for a long time, need to get up to speed quickly about procedures for handling information and dealing with requests. NSA has not done as good a job as it could in terms of documenting improvements in the procedures and instituting changes as a result of after action reports. We tend to pull together for a crisis and then pay only *pro forma* attention to the idea of preparing to respond better to the next crisis. We move onto other things after the crisis—these other things are important, but so too is the idea of preparing ourselves for the next NSOC iteration."

General Jobim thanked Dr. Coltrane and resumed leading the discussion. "In a crisis one of the central challenges is to cull the wheat from the chaff. It's the same in our daily operations. There is a staggering volume of communications traffic. Much of it is unencrypted; but thanks to our private sector friends in the information assurance business huge amounts of information are encrypted. How much of the encrypted stuff is important and who is it important to? Until we decode it, we probably can't know for sure.

"What I'm trying to tell you is that we have both a physical and an intellectual challenge. The physical challenge is intercepting signals and getting access to data. To do this we need to keep up with technological advances in computing, data storage and communications. The intellectual challenge is to go through the data and signals to cull out the important stuff. Often this involves both breaking sophisticated codes and translating foreign languages into English. Code breaking takes time, advanced computers and very smart crypto-analysts and linguists. Then once the codes are broken we need to determine the significance of the information."

"Right now we are upgrading our computers and communications gear and we have made the corporate decision to hire a contractor to manage the upgrade. Obviously, there is a lot riding on the upgrade. If the upgrade goes well, we should be reasonably well positioned for the future hardware-wise. In addition to hardware we also need to continuously upgrade and refresh our skill and knowledge base. Without smart mathematicians we won't be able to design the computer programs that break codes; without talented linguists and analysts we won't be able to make sense out of the information we get. I wish there were a private sector wizard we could hire to manage the upgrading of our people power; but there isn't.

"The information assurance folks like to tell people the four things that they need to be extremely good at in order to succeed. We in SIGINT also have four things on our 'must do well' list. First, we need to be exceptionally good at the physical act of collecting information. Second, because there is a vast flood of information out there, we need to be exceptionally good at sifting through the collected information to find the information that our customers might want. I use the word 'might' deliberately. Our customers think they know what they want today, but their needs change as crises evolve etc. Third, we need to be the best in the world at breaking codes. Fourth, we need to be able to convey our analyses to the right people, at the right time and in a manner that truly helps the customer. Of course, we need to be able to do each of these things well today and even better tomorrow."

After thinking about all of the information he had received during his research and interviews, Captain Basie decided to debrief Admiral Peterson. He thought it would be good to demonstrate to the admiral that he was making progress. He also wanted to make sure that he understood exactly what the admiral was expecting of him.

As the debriefing wound down, Basie sensed that Admiral Peterson was getting impatient. "Captain, it sounds like you have done a pretty good job, yourself, of collecting information. Now you know a lot about our two missions, information assurance and SIGINT. Your briefing has identified the key things the two directorates need to do well in order for the agency as a whole to succeed.

"So far, so good. But what I want you to do is to develop some recommended metrics that would tell us whether we are actually doing those key things as well as we should. I also want to hear your ideas about how we might measure our progress towards improving our capabilities in the future."

Notes

1. Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*, New York: Viking Books, 2001, p. 13-6.
2. Unless otherwise indicated, the material presented in dialogue form is drawn from interviews conducted by the author at the NSA in January 2001.
3. Chris Gaither, "Hacker Shuts Down Microsoft Sites", *New York Times*, 26 January 2001.
4. Transcript of CBS News broadcast, "National Security Nightmare", *60 Minutes II*, 13 February 2001, transcript accessed on the Internet on 14 February 2001, http//:cbsnews.com/now/story/0,1597,266857-412,00.shtml.
5. Seymour Hersh, "The Intelligence Gap: How the Digital Age Left Our Spies Out in the Cold," *The New Yorker*, 6 December 1999, p. 60-1.
6. Chuck McCutcheon, "Computer-Reliant U.S. Society Faces Growing Risk of Information War," *Congressional Quarterly Weekly Reporter*, Vol. 56, No. 11, 14 March 1998, pp. 675-9.
7. Chuck McCutcheon, "Pentagon's Simulated Attacks on Computers Succeed Too Well," *Congressional Quarterly Weekly Reporter*, Vol. 56, No. 24, 13 June 1998, pp. 1622-3.
8. Kurt Kleiner, "Spies Are US," *New Scientist,* 17 July 1999. Neil King, Jr., "NSA Chief Tries to Dispel Privacy Worries," *Wall Street Journal,* 13 April 2000. John Diamond, "Agency Denies Big Brother Charge; Accused of Spying on American Citizens, NSA takes Case to the Public," *Chicago Tribune*, 13 April 2000.